

## 1 Numbers

**Definition 1.** *Important sets of numbers.*

- $\mathbb{N} = \{1, 2, 3, \dots\}$  set of natural numbers,
- $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ ,
- $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$  set of integers,
- $\mathbb{Q} = \left\{ \frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{Z} \setminus \{0\} \right\}$  set of rational numbers,
- $\mathbb{R}$  set of all decimal expansions, set of real numbers.

**Definition 2** (Prime Number). *A prime number or prime is a natural number greater than one that is divisible by only one and itself.  $\mathbb{P} := \{p \in \mathbb{N} \mid p \text{ prime}\}$*

**Theorem 3** (Fundamental theorem of arithmetic). *Every positive integer  $n > 1$  can be represented in exactly one way as a product of prime powers:*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where  $p_1 < p_2 < \dots < p_k$  are primes and the  $\alpha_i$  are positive integers.

**Theorem 4** (Euclid). *There are infinitely many primes.*

**Definition 5** (axioms of real numbers). *Let  $x, y, z \in \mathbb{R}$ .*

### Axioms of addition

- *neutral element:*  $x + 0 = x$ ,
- *associativity:*  $(x + y) + z = x + (y + z)$ ,
- *commutativity:*  $x + y = y + x$ ,
- *inverse element:*  $y + (-y) = 0$ ;

## Axioms of multiplication

- *neutral element*:  $x \cdot 1 = x$ ,
- *associativity*:  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ ,
- *commutativity*:  $x \cdot y = y \cdot x$ ,
- *inverse element*:  $y \cdot \frac{1}{y} = 1$  for  $y \neq 0$ ;
- *distribution*:  $x \cdot (y + z) = x \cdot y + x \cdot z$ .

We write  $xy$  for  $x \cdot y$ ,  $x - y$  for  $x + (-y)$ ,  $y^{-1}$  for  $\frac{1}{y}$ ,  $\frac{x}{y}$  for  $x \cdot \frac{1}{y}$ ,  $x + x + \dots + x = nx$ , and  $x \cdot x \cdot \dots \cdot x = x^n$ . Furthermore, we define  $x^0 = 1$  for all  $x \in \mathbb{R}$ .

**Theorem 6** (Computation rules for powers). *If  $n, m \in \mathbb{N}_0$  and  $x, y \in \mathbb{R}$ , then*

- (i)  $x^n x^m = x^{n+m}$ ,
- (ii)  $x^n y^n = (xy)^n$ ,
- (iii)  $(x^n)^m = x^{nm}$ .

**Theorem 7** (Existence of non-rational numbers). *There exists no rational number  $x$  with the property that  $x^2 = 2$ .*

**Definition 8** (Ordering Axioms). *For all  $x, y \in \mathbb{R}$  we have  $x < y$  or  $x = y$  or  $y < x$  and these three possibilities are mutually exclusive. Moreover, for all  $x, y, z \in \mathbb{R}$  the relation  $<$  has the following properties:*

- a)  $x < y$  and  $y < z$  implies  $x < z$ .
- b)  $x < y$  and  $z > 0$  implies  $x + z < y + z$ .
- c)  $x < y$  and  $z > 0$  implies  $x \cdot z < y \cdot z$ .

**Definition 9** (Minimum/Maximum). *Let  $M \subset \mathbb{R}$  be a subset of the real numbers. An element  $x \in M$  is a minimum [maximum] of  $M$  if  $x \leq y$  [ $x \geq y$ ] for every element  $y \in M$ . We write  $x = \min M$  [ $x = \max M$ ].*

**Theorem 10** (Uniqueness of minima/maxima). *If both  $x$  and  $y$  are minima/maxima of a set  $M \subset \mathbb{R}$ , then  $x = y$ .*

**Definition 11** (Absolute value). *The absolute value or modulus of a real number  $x$  is defined by*

$$|x| = \begin{cases} x & \text{for } x \geq 0 \\ -x & \text{for } x < 0 \end{cases}.$$

**Theorem 12** (Properties of the absolute value). *Let  $x, y \in \mathbb{R}$ . Then*

- $|x| \geq 0$  and  $x = 0$  precisely if  $x = 0$ ,
- $|xy| = |x||y|$ , in particular  $|x| = |-x|$ ,
- $|x + y| \leq |x| + |y|$  (triangle inequality),
- $-|x| \leq x \leq |x|$ ,
- if  $|x| \leq y$ , then  $-y \leq x \leq y$ .

**Definition 13** (Negative powers). *For  $n \in \mathbb{N}$  and  $x \in \mathbb{R} \setminus \{0\}$  we define*

$$x^{-n} = (x^{-1})^n = \frac{1}{x^n}.$$

**Theorem 14** (Existence of roots). *For  $n \in \mathbb{N}$  and  $x > 0$  there is a unique number  $y > 0$  such that  $y^n = x$ .*

**Definition 15** (Roots). *In the situation of Theorem 14, we define*

$$y = x^{\frac{1}{n}} = \sqrt[n]{x}$$

*and call  $y$  the  $n$ -th root of  $x$ . For  $p, q \in \mathbb{Q}$ ,  $q \neq 0$ , we define*

$$x^{\frac{p}{q}} = (x^{\frac{1}{q}})^p.$$

**Proposition 16** (Squares are positive). *If  $x \in \mathbb{R} \setminus \{0\}$ , then  $x^2 > 0$ .*

**Definition 17** (Sums & Products). *For  $n, m \in \mathbb{Z}$  with  $m \leq n$  and  $a_m, a_{m+1}, \dots, a_n \in \mathbb{R}$  we define*

$$\sum_{k=m}^n a_k = a_m + a_{m+1} + \dots + a_n,$$

$$\prod_{k=m}^n a_k = a_m \cdot a_{m+1} \cdot \dots \cdot a_n.$$

## Complex Numbers

In mathematics, we do a lot of solving of polynomial equations, which amounts to finding a root of a polynomial. For example, the solutions to the equations  $x^2 = 1$  are the same as the solutions of  $x^2 - 1 = 0$ , that is, they are the roots of the polynomial  $x^2 - 1$ . These roots are  $x = 1$  and  $x = -1$ . However, some polynomial equations have no real number solutions: for example, the equation

$$x^2 + 1 = 0$$

has no real number solutions, because  $x^2 + 1 \geq 1$  if  $x$  is a real number. The complex numbers were invented to provide solutions to polynomial equations.

**Definition 18.** A complex number is a number  $z$  of the form  $z = x + iy$ , where  $x$  and  $y$  are real numbers, and  $i$  is another number such that  $i^2 = -1$ . The set  $\mathbb{C}$  of complex numbers is defined as

$$\mathbb{C} = \{(x, y) : x, y \in \mathbb{R}\}$$

together with an addition and multiplication:

$$\begin{aligned}(x, y) + (u, v) &= (x + u, y + v), \\ (x, y) \cdot (u, v) &= (xu - yv, xv + yu).\end{aligned}$$

For the imaginary unit  $i = (0, 1)$  we have  $i^2 = (-1, 0)$ .

$$z = x + iy, \quad x, y \in \mathbb{R}$$

is the standard description of complex numbers  $z \in \mathbb{C}$ . We call

$$\operatorname{Re} z = x \text{ and } \operatorname{Im} z = y$$

the real and imaginary part of  $z$ . The complex conjugate of  $z$  is defined by

$$\bar{z} = x - iy = \operatorname{Re} z - i\operatorname{Im} z.$$

With the above definitions we have

$$\begin{aligned}z + \bar{z} &= 2\operatorname{Re} z, \\ z - \bar{z} &= 2i\operatorname{Im} z, \\ z \cdot \bar{z} &= (x + iy)(x - iy) = x^2 + y^2 \in \mathbb{R}.\end{aligned}$$

**Theorem 19.** All axioms regarding sums and products in  $\mathbb{R}$  carry over to  $\mathbb{C}$ . In particular,

- (i) addition is commutative and associative;
- (ii) multiplication is commutative and associative;
- (iii) the distributive law relating addition and multiplication holds;
- (iv) for every  $z \in \mathbb{C}$ :  $z = z \cdot 1 = z + 0$  and  $z \cdot 0 = 0$ .

**Definition 20.** The distance of a complex number  $z$  from the origin is called modulus, length or absolute value of  $z$  and is given by

$$|z| = \sqrt{(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2} = \sqrt{z\bar{z}}.$$

**Theorem 21.** For  $z, w \in \mathbb{C}$ :

- a)  $|z| = |-z| = |\bar{z}|$ ;
- b)  $|z| \geq 0$  and  $|z| = 0$  iff  $z = 0$ ;
- c)  $|zw| = |z||w|$ ;
- d)  $||z| - |w|| \leq |z + w| \leq |z| + |w|$ .

**Theorem 22.** For  $0 \neq z = x + iy$ :

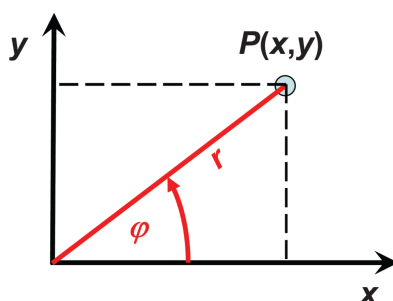
$$(x + iy) \frac{x - iy}{x^2 + y^2} = 1.$$

Hence, the denominator of a quotient  $\frac{z}{w}$  can be made a real number by multiplication with  $\frac{\bar{w}}{\bar{w}}$ .

**Theorem 23.** For  $z \in \mathbb{C}$  there exist real numbers  $r \geq 0$  and  $\varphi \in \mathbb{R}$  with

$$z = r(\cos \varphi + i \sin \varphi).$$

We always have  $r = |z|$ , and for  $z \neq 0$ , the number  $\varphi$  is uniquely determined by the condition  $-\pi < \varphi \leq \pi$ . The pair  $(r, \varphi)$  are the polar coordinates of  $z$ , and  $\varphi$  is called the argument of  $z$ , denoted by  $\arg z$ .



**Theorem 24.** For  $\varphi \in \mathbb{R}$ :

$$e^{i\varphi} = \exp(i\varphi) = \cos \varphi + i \sin \varphi.$$

**Theorem 25.** For complex numbers  $z_1 = r_1 e^{i\varphi_1}$  and  $z_2 = r_2 e^{i\varphi_2}$ :

$$z_1 \cdot z_2 = r_1 r_2 e^{i(\varphi_1 + \varphi_2)}.$$

**Theorem 26** (Formula of DE MOIVRE). For  $n \in \mathbb{N}$  and  $w \in \mathbb{C} \setminus \{0\}$  there exist exactly  $n$  different solutions of the equation  $z^n = w$  given by

$$z_k = \sqrt[n]{|w|} e^{i \frac{\psi + 2k\pi}{n}}, k = 0, 1, \dots, n-1,$$

where  $\psi = \arg w$ .

**Theorem 27** (Fundamental Theorem of Algebra). Every polynomial with coefficients in  $\mathbb{C}$  has a root in  $\mathbb{C}$ .